Changing the World: IoT Chaos as a Ladder to Improving Security

The ISO/OCF Standard and Implementation for Security

A Technical Paper prepared for SCTE•ISBE by

Brian A. Scriber
Distinguished Technologist and VP of Security Technologies
CableLabs
858 Coal Creek Circle, Louisville, CO 80027
@brianscriber
b.scriber@cablelabs.com

Table of Contents

List of Figures

Introduction

With each device on our networks vulnerable to attack with processing/memory/storage and network credentials, how can we help to protect consumers, the network and other participants? How do we raise the security tide for all boats? How do we attack the economic problem here while we work the technical issues? If an entrepreneurial CTO is ever asked by his CFO or CEO "How much is security going to cost me?" we've already lost. The Open Connectivity Foundation (OCF) is an organization of over 450 companies, with several SCTE member companies actively participating and a couple serving on the Board of Directors. OCF is working together to not only write the specifications for interoperability and security, but also build out an entire open-source (as in free) implementation of this specification (IoTivity) to help even the most cash-strapped start-up build secure IoT software. Join us to learn the current state of OCF, IoTivity, certification and how you can get started changing the world of IoT security.

Changing the World

IoT Security has an economics problem. There is a misalignment between incentive structures with respect to the externalites of botnet attacks. It takes an investment of time and money for manufacturers to secure devices and for manufacturers to update a device they have already sold, it pulls directly from their bottom line; this is a tangible disincentive for manufacturers to address problems caused by insecure devices. The victims of botnet activity, Distributed Denial of Service (DDoS) attacks, and other malicious traffic are not those manufacturers; those costs are born by downstream inhabitants of the IoT ecosystem.

Those effects impact consumers, governments, network operators, and any target of a DDoS attack. The economic burden of such an attack on a retail site averages between $20,000 and $40,000 per hour[i], however the cost to hire a 100Mbps attack for an hour is roughly $5[ii]. The ability to rent botnets stems from the raw number of devices available for malicious actors to compromise as well as the ease of compromise of connected devices with little or no security (botnets Torii, Demonbot, Mirai/clones, and Chalubo all heavily leverage IoT). There are roughly 8 connected devices per person on the planet in 2019 with a 50% growth expected over the next three years. That disparity between the ease of attack and damage from an attack, times the 793,377 attacks through cable networks in 2018[iii,iv] is the economic burden of insecure devices.

1. IoT Security Misconceptions

The major parts of this problem come from the realities of the niche smart home electronics manufacturers occupy and a few erroneous assumptions about IoT include the following:

- **Misconception #1: "Device pricing is the only mechanism available for differentiation against competition."** However, as Apple has shown in 2018 and 2019[v], device security can be a differentiator and buyers will make decisions based on how well devices protect their investments.
- **Misconception #2: "Security isn't important for end users."** However, security is cited within the top three buying concerns[vi] and has an influence on 75% of IoT consumers[vii].
- **Misconception #3: "Security is about the protection of the device"** Concerns raised in discussions around IoT Security in relation to the NIST direction on IoT[viii,ix] continue to return to classes of device with a desire to create different security levels for different device types. The argument is that a lightbulb or a connected Barbie® doll don't require the same security as other devices. The reality is that those devices have a processor, memory, power, a network stack, and

networking credentials that the owner provided which make each of them an ideal launching point for further attacks[x] and make them excellent participants in the botnets that have garnered legislative attention. Regulators have no motivation to care about the device being compromised if that's where it ended, they care about this sector of the economy because botnets using those devices are the weapons that can take down strategic infrastructure. It isn't about the device, it's about the network; it's always been about the network.

2. How Can We Fix This?

The quick answer, the one that falls into Mencken's "neat, plausible, and wrong"[xi] category is that we can just create a specification for IoT devices, make it a standard and everyone will use it. The trick here is that IoT isn't as simple as the three letter acronym makes it appear, these devices are actually computers, some with more or less resources than others, but they have operating systems, drivers, radios, networking stacks, layers of code libraries, processors, memory, power needs, some have cryptographic coprocessors and Trusted Platform Modules (TPMs), others are general purpose computers with small form factors. Writing a specification that doesn't take this into consideration is a recipe for failure.

Even with an agreed-upon specification, adoption of that specification by the global manufacturing community is another cognitive leap that takes a measure of suspension of disbelief. The real trick to this, however, is the entrepreneurial company that has decided to build a connected device. They may not have a cryptographer on staff, they may not have a network security expert or even a networking expert; this company may outsource the entirety of their development to other lowest-bidder firms where simple hardware and old software are combined to provide the Minimum Viable Product (MVP) for launch of the idea. This MVP likely has no consideration for security, the company releasing it may not know all the code libraries used, the versions, the vulnerabilities for each version, or even have applied it to the correct hardware. Permissions are likely granted through hard-coded credentials and as the mirai botnet leverages, those passwords are easy to try in series because no effort to limit unsuccessful attempts is ever engaged. This entrepreneurial company has no interest in reading a 200 page security specification let alone comply with that for what they consider a novel product with perceived market pressures and investors who follow Eric Reis's Lean Startup methodology driving them to release as quickly and as early as possible. The prevalence of botnets shows that addressing security isn't always treated as a priority in this environment.

3. Entrepreneurial Incentives

Even if security is brought up at this hypothetical entrepreneurial company, if it were to negatively impact a schedule or if it led to additional costs, a conversation between the CFO or CEO would ensue about those impacts. If this conversation happens, without an answer of "security is free" or "it would cost us extra time or money to *remove* security from the software", the result is a less secure product. When it comes to product security, it is for the perceived cost of security, that specifications alone cannot satisfy the market; specifications must be accompanied by implementation software that is free-to-use, modifiable, reviewed, and preferably open-source.

The OCF is such a combination; it includes a detailed security specification and has IoTivity, a separate, Linux Foundation managed, open source implementation of that specification available for use without cost. The added incentive from the OCF is that in using this specification/software, the product created will be interoperable with the IoT product lines from other members of the OCF which include over 450 of the world's most influential and prolific manufacturers including Intel, Shaw, Samsung, LG, Microsoft, Electrolux, Cox, Haier, Comcast, Qualcomm, Charter, Cisco, and others. Now, an entrepreneurial firm has the incentive to use the IoTivity code because it solves many of their non-application layer concerns. They are incented because they know that IoTivity is built with security which includes device identity, confidentiality of messages, access control, and strong authentication. The are also incented because they now know that they have the door open for interoperability with product lines from the hundreds of OCF member companies. This is the argument that wins over not just the large players in the IoT space, but provides cover for all of the entrepreneurial companies as well. This is how security becomes part of the foundation for an ecosystem.

The Open Connectivity Foundation Security Specification

4. The OCF Network

OCF is a Layer-4 and Layer-5 technology, it is transport agnostic and can run on WiFi, Bluetooth, Thread and efforts are underway for other transports. As new OCF Devices are introduced to this network, the Device Ownership Transfer Service (DOTS – aka "onboarding tool") broadcasts a discovery message to which the OCF Device responds. The DOTS then interrogates device credentials and, through the Credential Management Service (CMS) issues new local OCF-network credentials to the device. Through the Access Management Service (AMS) the DOTS then establishes and enforces access control to the Resources within the Device. Resources are collection of related Attributes that follow the OCF Data Model. Access to a Resource is limited through Create, Read, Update, Delete, and Notify (CRUDN) operations stored in Access Control Entries (ACE) within the Access Control List (ACL) aspect of the AMS. This allows Devices to interact with other proximal devices and engage in a Scenes or Rules to enable advanced functions like "vacation mode" where lights turn on at sporadic intervals and curtains raise and lower accordingly.

4.1. Network Provisioning

Because OCF is a Layer-4/Layer-5 technology, there is a presumption that the Device has been onboarded into the network where it can receive multicast messages from the DOTS. With WiFi, the WiFi Alliance (WFA) has a Device Provisioning Protocol (DPP) for securely introducing the Device to the WiFi network and provisioning it with credentials to receive additional instructions from OCF. The OCF, the WFA, and CableLabs, are engaged in making this a seamless transition and effortless for the user.

5. Onboarding Detail

Onboarding has three distinct phases: Discovery, Ownership Transfer, Provisioning, and Normal Operation.

5.1. Discovery

In the Discovery phase of onboarding, the DOTS sends a multicast discovery message which is not encrypted. Devices receiving this message, which have not been "owned" reply directly to the DOTS. The reply message includes the list of methods by which the Device can communicate through the ownership transfer – these methods are called Ownership Transfer Methods (OTM). The currently supported OTMs include the "Just Works" Authenticated Diffie Hellman exchange, the Pre-Shared Key symmetric cryptographic exchange, and Certificate Based Onboarding. The Certificate-Based Onboarding OTM has a "Baseline" which is equivalent to a self-signed certificate and then additional optional "profiles" for enhanced Device identity protection.

- **Purple**: The "purple" profile makes (unverified, but attested to) claims about the capabilities of the device (e.g. that there is a Secure Execution Environment (SEE)).

- **Blue**: The "blue" profile relies upon the DOTS to optionally check on the current certification status for the Device based on the make and model of the Device through an online certification verification system.
- **Black**: The "black" profile requires that Devices have passed the OCF testing protocol at one of the Approved Test Labs (ATL) before it is issued a digital certificate which is part of the official OCF Public Key Infrastructure (PKI). The certificate for the Device chains to one of the approved Certificate Authorities who can only issue certificates in accordance with the Certificate Policy defined by OCF for compliant devices.

The supported OTMs might include multiple methods to acceptably onboard the Device. The decision about which OTM to select is the prerogative of the owner of the network through the DOTS.

5.2. Ownership Transfer

There are three steps in the Ownership Transfer process:

1. The DOTS, having received the OTMs supported, selects the OTM and configures that OTM to the Device – this interaction is also over an unsecured channel.
2. DOTS and the unowned Device perform the OTM using the credentials associated with the OTM. Part of this exchange is the establishment of the TLS handshake.
3. DOTS configures the Security Virtual Resources (SVRs) of the Device, the CMS and the AMS to authorize itself for further provisioning of the Device. These secure interactions occur over TLS.

At this point, the Device is "owned" by the DOTS and the Ownership Transfer is complete.

5.3. Provisioning

The two steps involved in provisioning for the Device are the creation of credentials and the establishment of access control properties.

The CMS issues credentials to the Device, currently both symmetric and asymmetric credentials are supported, but the preference is toward asymmetric to support Role Based Access Control (RBAC) which is discussed later. Interactions with the CMS are under secure communications using TLS.

The AMS provisions the access control policies for the Device, creating ACEs for each relationship with other Devices that are to be granted access for reading, notification, or setting of attributes using the CRUDN ACE for the ACL. All interactions with the AMS require secure communications using TLS.

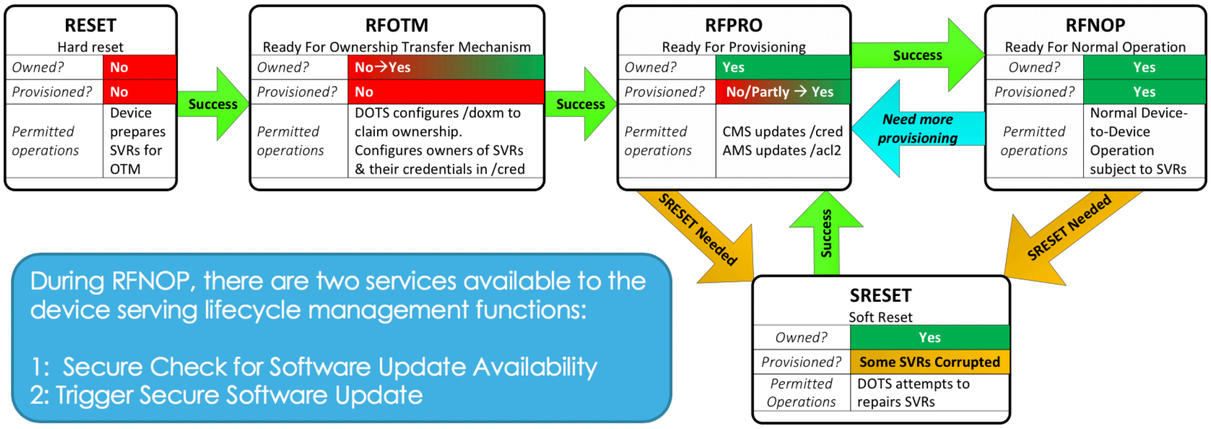
At this point, the Device is provisioned with credentials for the OCF Network and has been granted the access it needs to be effective, it is now ready for Normal Operation.

5.4. Normal Operation

During Normal Operation, the Device acts within the access control granted through the AMS using the credentials it was issued by the CMS. Should either of these require changes, the Device returns to Provisioning.

6. State Transitions for OCF Devices

In the Onboarding Detail section, some implied state transitions for the Device occur; this section explores those at a greater level of detail. Figure 1 - Device Provisioning States explores these state transitions.


RESET
Hard reset
Owned? No
Provisioned? No
Permitted operations
Device prepares SVRs for OTM
Success
RFOTM
Ready For Ownership Transfer Mechanism
Owned? No→Yes
Provisioned? No
Permitted operations
DOTS configures /doxm to claim ownership. Configures owners of SVRs & their credentials in /cred
Success
RFPRO
Ready For Provisioning
Owned? Yes
Provisioned? No/Partly → Yes
Permitted operations
CMS updates /cred AMS updates /acl2
Success
Need more provisioning
RFNOP
Ready For Normal Operation
Owned? Yes
Provisioned? Yes
Permitted operations
Normal Device-to-Device Operation subject to SVRs
SRESET Needed
Success
SRESET Needed
SRESET
Soft Reset
Owned? Yes
Provisioned? Some SVRs Corrupted
Permitted Operations
DOTS attempts to repairs SVRs

During RFNOP, there are two services available to the device serving lifecycle management functions:

1: Secure Check for Software Update Availability
2: Trigger Secure Software Update

Device can transition to ***RESET*** *from any state (these transitions are not shown)*

Figure 1 - Device Provisioning States

6.1. RESET

The Reset state is the original state the device came from out of the box, or as close to that state as possible if it arrives back at that point through a factory-reset or “hard reset”. Initial identity credentials such as the digital certificate issued to the device by the manufacturer are unchanged in a transition back to this state, but all local credentials are removed from the Device.

6.2. Ready For Ownership Transfer Method (RFOTM)

RFOTM can be transitioned to only from the RESET state. The action taken during this transition is the preparation for the security resources (SVRs) to be established which is likely already the case in RESET.

Transitioning out of RFOTM is the Ownership Transfer described in section 5.2. If it is successful, the Device transitions to RFPRO, but if the Ownership Transfer is unsuccessful, the Device sets its “Owned” status to false, deletes any credentials other than the initial identity credentials, resets any other Resources to their defaults and transitions back to RESET.

6.3. Ready For Provisioning (RFPRO)

RFPRO can be transitioned to from three different states: the RFOTM during initial onboarding, from SRESET during a partial update, and from RFNOP if additional credentialing or access management need to be provisioned for the Device. In all of these cases the “Owned” status remains true.

Transitioning out of RFPRO also can go to three different states. In the nominal case, after the provisioning of credentials with the CMS and provisioning of access management with the AMS occur (as described in section 5.3), the Device transitions successfully to the RFNOP state. In the case where there are errors with the SVRs, and if those errors are potentially recoverable, the Device transitions to the SRESET state to hopefully remedy any issues. If the errors persist or are irrecoverable, the Device transitions to the RESET state with the accompanying loss of local credentials and a reset to default Resource values.

6.4. Ready for Normal Operation (RFNOP)

RFNOP is the nominal state for a Device after it has been through onboarding. This is the state for normal operation and, in a perfect world, where the Device will spend the majority of its time. Transitioning to RFNOP can **only** be accomplished through successful provisioning and a transition directly from RFPRO.

Transitions from RFNOP are to SRESET in the case of corrupted SVRs that may be recoverable, and also transition back to RESET if the corruption requires a hard reset. It is also possible to transition from RFNOP to RFPRO when either new credentials or new access control is required as those can only be granted to Devices in the RFPRO state.

6.5. Soft Reset (SRESET)

The SRESET state exists to prevent complete reworking of all of the credentialing and access management assigned to the Device. It carries some inherent risk because there is no way to determine exactly how the corruption may have occurred. The SRESET state is managed by the DOTS, which is controlled by the owner of the OCF Network. If the owner prohibits the SRESET state, any transition to this state transitions directly to RESET instead, including all of the requisite resetting of credentials and access control. It is possible to transition to SRESET from either RFPRO or RFNOP.

Transitioning out of SRESET to RESET can happen either through the policy as described above, or through a failed attempt to restore SVRs through the DOTS. If the SVRs can be restored successfully through the DOTS the Device can transition to only the RFPRO for verification and any refinements to either the credentials installed in the CMS or to the access control granted through the AMS.

7. Access Control

Access Control limits the Smart Toaster from opening the Smart Lock on the front door. It is critical in an ecosystem and the entire network can be compromised if the access control isn’t part of the design from the very start.

7.1. ACEs and ACLs

Devices have Resources, and each of those Resources are protected by an ACE. The ACE allows another Device the ability to act on the Resource with different granted permissions: Create, Read, Update, Delete, and Notify. Most of these are self-explanatory, but Notify can be thought of as a perpetual Read where the reader is advised of changes made to the Resource. **All** requests to any of a Device’s Resources are subject to the ACL policy verification where the appropriate ACE is evaluated. A simple overview of a successful Read on a Device and an unsuccessful Update is shown in Figure 2 - Access Control Example.

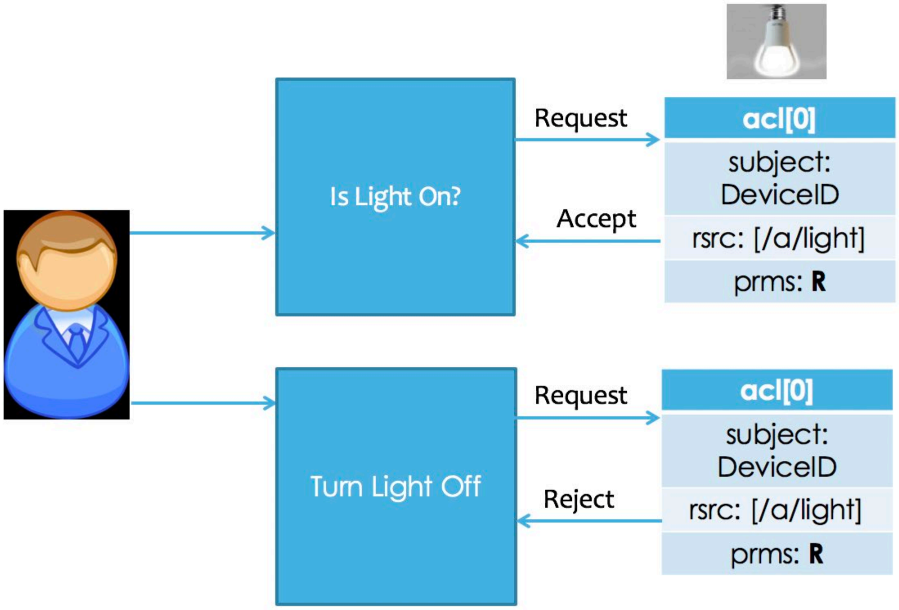


Figure 2 - Access Control Example

7.2. Access Control Types

There are two types of access control, Subject-Based Access Control (SBAC) and Role-Based Access Conbtrol (RBAC).

In the SBAC approach a single Device is given the ability to perform actions specified by the CRUDN options and recorded in the ACE. The Device is named by the network identity of that Device assigned at onboarding time.

In the RBAC approach the ACE specifies the Role permitted to perform the CRUDN operations. The Role can them be assigned to any of the appropriate Devices. An example of this might be Temperture Sensors that allow anything with the Thermostat Role to read different temperature Resources.

7.3. Access Management Service

The Access Manager Service (AMS) is the only mechanism for updating ACE/ACLs. To ease deployment options and to make some communications methods easier, wildcarding of permissions was added to the model.

It is important to note that permissions are checked inbound to Resources – OCF does not currently have outbound ACLs restricting a Device from attempting a specific communication, it relies on the ACE of the Resource being requested to check permissions.

8. Message Integrity and Confidentiality

Within the onboarded OCF network, all unicast messages are secured using TLS or DTLS. Multicast messages are not secured, but also do not have a requirement that Devices respond to, or consume, the multicast messaging. All unicast messages are signed, ordered, and encrypted. This protects against eavesdropping on message contents, tampering with messages, and replay attacks.

8.1. Credential Management Service

In order for Devices to have this level of communication protection, the Devices must have usable credentials. Those credentials are assigned in the RFPRO state before the Device is in the RFNOP state associated with normal operation. When the credential expire, or if new credentials need to be provisioned, the Credential Management Service (CMS) installs or renews as necessary and in compliance with the policy defined by the network owner.

Conclusion

The Kaizen[xii] approach of asking the five whys helps to drive the understanding of IoT Security and how to change it. **Why** are legislators looking at regulating IoT? Because our networks are being attacked. **Why** is that? Networks are being attacked because of the ease and availability of attack platforms. **Why** are these platforms so inexpensive? Attack platforms are comprised of the prolific deployment of low-security IoT devices. **Why** are these prone to attack? Because there is an economic disincentive to manufacturers to design these devices with security in mind and to update to defend against new threats. **Why** can't we unwind this disincentive? The economics of adding security at the point of design adds cost, the consumer cannot adequately differentiate between the security provided by different products, and different devices are challenged by not "speaking the same language" let alone share a common security paradigm.

The answer to those three primary drivers are the primary forces that brought together 450+ major manufacturers to create the Open Connectivity Foundation. The three problems each have a pillar in the structure of OCF:

1) **Interoperability**: OCF provides a common data model for Devices and a set of rules for how device security needs to interact. Devices must have a unique, attestable, immutable identifier used to onboard into the network; communication is secured via TLS to guarantee message integrity and confidentiality; access is controlled at the Resource level and Device integrity is managed through clearly defined state transitions.
2) **Cost of Security**: Through building not just a specification, but an actual implementation of that specification, and then providing that implementation without cost through the Linux Foundation's open source project, IoTivity, the OCF has created an architecture with security as a primary design consideration. This creates a world where it actually costs more if an entrepreneurial company wanted to build a product without security considerations.
3) **Consumer Education**: The OCF and their Approved Test Labs which certify compliance of the Devices against a rigorous framework to check alignment with the specification. This logo enables the consumer to know that, if the OCF label appears on the box, the Device inside has passed all of the security compliance and interoperability tests approved by the OCF.

This is the beginning of the real value and climb out from the IoT insecurity morass. The work isn't over, there will still be improvements made and there are still millions of insecure devices currently deployed, but these are steps in the right direction and the hope is that we will see the tide rise for all boats as the tools have now been made available.

Abbreviations

ACE	access control entry
ACL	access control list
AMS	access management service
ATL	Approved Test Laboratory

CMS	Credential Management Service
CRUDN	Create/Read/Update/Delete/Notify access control permissions
DOTS	Device Ownershipo Transfer Service
DPP	Device Provisioning Protocol (WiFi Alliance)
OBT	Onboarding Tool
OCF	Open Connectivity Foundation
OTM	Ownership Transfer Methods
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
SEE	Secure Execution Environment
SVR	Security Virtual Resources
TPM	Trusted Platform Module
WFA	WiFi Alliance

Bibliography & References

ISO/IEC 301 18-1:2018 Information Technology – Open Connectivity Foundation (OCF) Specification – Part 1: Core specification https://www.iso.org/standard/53238.html

[i] https://www.coxblue.com/12-ddos-statistics-that-should-concern-business-leaders/

[ii] CableLabs: Survey of Dark Web Activity, most recently verified, March 2019

[iii] https://securelist.com/ddos-report-q1-2019/90792/

[iv] NETSCOUT Threat Intelligence Report 1H 2018

[v] https://www.techtimes.com/articles/239693/20190314/apples-new-iphone-ad-shows-how-much-privacy-matters.htm

[vi] Open Connectivity Foundation primary research, 2017

[vii] https://www.cs.cmu.edu/~pemamina/publication/CHI'19/CHI19.pdf

[viii] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

[ix] https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

[x] https://www.cablelabs.com/just-lightbulb-need-security

[xi] “Explanations exist; they have existed for all time; there is always a well-known solution to every human problem — neat, plausible, and wrong.” – H.L. Mencken, "The Divine Afflatus" in *New York Evening Mail* (16 November 1917); later published in *Prejudices: Second Series* (1920) and *A Mencken Chrestomathy* (1949)

[xii] https://en.wikipedia.org/wiki/Kaizen